

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v-

LILIA BARNES,

Defendant.

X
:
:
:
:
:
:
:
:
:
:
X

13 Cr. 387 (AJN)

MEMORANDUM &
ORDER

ALISON J. NATHAN, District Judge:

Before the Court are Defendant Lilia Barnes’s pre-trial motions to suppress evidence seized from two email accounts and to compel the Government to produce a bill of particulars. For the following reasons, Barnes’s motions are denied.

I. BACKGROUND

The Workforce Investment Act of 1998 (“WIA”), 29 U.S.C. § 2801 *et seq.*, provides federal funds to state and local workforce investment boards, which offer job training programs that “improve the quality of the workforce, reduce welfare dependency, and enhance the productivity and competitiveness of the Nation.” *Id.* § 2811. In New York, the state investment board has authorized local boards, including the New York City Workforce Investment Board (“NYC-WIB”) to implement such federally funded job training programs at the local level. Compl. ¶¶ 8(b)–(c). One of these local programs is “Workforce1,” which operates career centers throughout the five boroughs. *Id.* ¶ 8(d). Among other things, Workforce1 centers approve applications for educational vouchers, which allow students to receive job training paid for by funds from NYC-WIB. *Id.*

Barnes operates the L & Barnes Driving School (“L&B”) in Manhattan, which accepts educational vouchers funded by NYC-WIB. Def. Br. at 1. The Complaint alleges that between 2009 and 2012, Barnes participated in a “kickback scheme” in which Workforce1 employees referred voucher recipients to L&B in exchange for cash payments made by Barnes through an intermediary. Compl. ¶ 11(a).

On May 22, 2013, Barnes was indicted on one count of conspiracy to commit bribery in violation of 18 U.S.C. §§ 666(a)(1)(B) and (a)(2). Harris Decl. Ex. B. On May 31, 2013, the Government sought search warrants for two email accounts associated with L&B. The application for the warrants was filed by Christopher Wilson, a Special Agent with the Department of Homeland Security. Harris Decl. Ex. C ¶ 2. The application contained background information about Barnes’s alleged crimes, and the Complaint was attached to it as Exhibit A. With respect to the two target email accounts, the application stated that one of the accounts, liliatrucks@yahoo.com (the “Yahoo Account”), was listed as L&B’s email address on documents that L&B had submitted to the New York State Department of Labor (“DOL”) to establish the business’s eligibility for WIA funds. *Id.* ¶ 18. The second account, barnesdrivingschool@gmail.com (the “Google Account”), was listed on L&B’s website—as of May 30, 2013—as L&B’s email address. *Id.* ¶ 19. The warrant application also indicated that L&B’s website had a scroll that referenced “GOVERNMENT PROGRAMS,” “WORKFORCE,” and “ITA VOUCHERS, etc.” *Id.*

Additionally, the warrant application contained details about the two-step procedure by which the Government planned to execute the warrants. Barnes Decl. Ex. C ¶¶ 24–29. Specifically, the government would first obtain a digital copy of the two email accounts from Yahoo and Google, the Internet Service Providers (“ISPs”) who hosted the accounts. *Id.* ¶ 27.

Government agents would then search those copies for the specific information that the warrants authorized to be seized. *Id.* The agents' search would take place off-site to avoid impacting the ISPs' business operations, *id.*, and would "require that agents cursorily inspect all information from the accounts in order to ascertain which items of information contain evidence of [Barnes's alleged] crimes, just as it is necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine which documents fall within the scope of the warrant," *id.* ¶ 25.

On May 31, 2013, the Honorable Ronald L. Ellis, United States Magistrate Judge, issued two warrants authorizing the seizure of the Yahoo Account and the Google Account, respectively. Harris Decl. Ex. D. The warrants both have three sections, and except for ISP-specific information, they are identical. First, they list the "[p]roperty to [b]e [s]earched," which in both cases are business addresses where the ISPs stored the information associated with the two accounts. Second, the warrants list "[i]nformation to be disclosed" by the ISPs, which consists of "[a]ll stored electronic mail and other stored content information presently contained in, or on behalf of," the two accounts, in addition to the entirety of certain categories of non-content information¹—in other words, essentially all of the information in and associated with the accounts, including all emails. Third, the warrants list "[i]nformation to be seized by the Government." The information subject to seizure by the Government consists of "[a]ll information described above" (*i.e.*, in the disclosure section of the warrants) "that constitutes

¹ The Court uses these rough categories—"content" and "non-content"—to avoid quoting at length from the warrants' descriptions of information subject to disclosure. Generally, "In the case of e-mail . . . the subject line, the body of the message, and any attachments count as the contents of the communication. They are the actual message to be sent. Everything else in the e-mail, including the to/from address and the size of the e-mail, counts as non-content information." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1030 (2010). The warrants also required the ISPs to disclose certain subscriber information.

fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 and 666, including” content and non-content information in five specified categories.

On August 30, 2013, Barnes filed the instant motions. Dkt. No. 25.

II. DISCUSSION

Barnes asks the Court to suppress any evidence seized on the authority of the two search warrants and to compel the Government to produce a bill of particulars. The Court addresses her motion to suppress first.

A. Barnes’s Motion to Suppress Is Denied

In arguing for suppression, Barnes challenges the sufficiency of the warrants authorizing the search of the two email accounts. The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. A warrant must therefore both be supported by probable cause and set out the scope of the authorized search and seizure with particularity. *See Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). Barnes challenges the warrants along both of these dimensions.

1. The Warrants Were Supported by Probable Cause

Probable cause exists when there is a “fair probability that the premises will yield the objects specified in the search warrant.” *United States v. Muhammad*, 520 F. App’x 31, 38 (2d Cir. 2013) (quoting *United States v. Travisano*, 724 F.2d 341, 346 (2d Cir. 1983)) (internal quotation mark omitted); *see also Illinois v. Gates*, 462 U.S. 213, 238 (1983). Thus, there must be a “nexus between the items sought and the ‘particular place’ to be searched.” *United States v. Clark*, 638 F.3d 89, 95 (2d Cir. 2010) (quoting *Stanford v. Texas*, 379 U.S. 476, 481 (1965)). “A showing of nexus does not require direct evidence and ‘may be based on “reasonable inference”

from the facts presented based on common sense and experience.” *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004) (quoting *United States v. Buck*, No. 84 Cr. 220 (CSH), 1986 WL 12533, at *4 (S.D.N.Y. Oct. 24, 1986), *rev’d on other grounds*, 813 F.2d 599 (2d Cir. 1987)); *see also Travisano*, 724 F.2d at 346 (“[I]t is only a probability, and not a prima facie showing of criminal activity, that is the standard of probable cause.”). Additionally, the Supreme Court has “repeatedly said that after-the-fact scrutiny by courts of the sufficiency” of a warrant application “should not take the form of *de novo* review. A magistrate’s ‘determination of probable cause should be paid great deference by reviewing courts.’” *Gates*, 462 U.S. at 236 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)).

Barnes argues there was no “nexus” between the objects specified in the search warrant—evidence of her alleged crimes—and the two accounts. Def. Br. at 8. The Court disagrees. The warrant application sufficiently established that the accounts likely contained communications regarding voucher programs; those communications constitute relevant evidence of the charged kickback scheme by tending to make the *mens rea* element of Barnes’s alleged crimes more likely.

With respect to the Yahoo Account, the warrant application stated that L&B had listed the account as its email address on DOL records concerning L&B’s eligibility for WIA funds. Harris Decl. Ex. C ¶ 18. While the Government submits that “the mere fact that the Yahoo Account was a business account . . . , combined with the facts establishing the offense and the business’s involvement in it, is sufficient” to establish probable cause to search the account, Gov. Opp. at 6, Barnes disagrees. If the Government’s argument were correct, she claims, then a warrant to search the office of a business suspected of criminal activity “could issue based only on the indictment accompanied by a sworn statement of the business’s address.” Def. Reply at 2.

Whether or not Barnes is right about the implications of the Government's argument, the facts here are not actually as stark as she suggests. The Yahoo Account was not just L&B's business account but was also listed on paperwork specifically concerning the voucher program involved in the charged kickback scheme. It would thus be reasonable to conclude that communications by L&B concerning that program would be found in the account. *Cf., e.g., United States v. Vilar*, No. 05 Cr. 621 (KMK), 2007 WL 1075041, at *20 (S.D.N.Y. Apr. 4, 2007) (noting that allegations of wrongdoing involving an investment advisor "[c]learly" provided "probable cause to conduct some form of search of the [advisor's] offices"); *United States v. Taormina*, No. 97 Cr. 1120 (MBM), 1998 WL 702341, at *2 (S.D.N.Y. Oct. 8, 1998) (concluding that evidence that defendant had made an unlawful payment "was enough to justify the conclusion that a search of [his] business office might disclose documents reflecting the payment, [his] obligation to make further payments, and the reason for such payments").

Even if the warrant application did demonstrate a link between the Yahoo Account and the voucher program, Barnes argues next, it contained nothing establishing that "evidence of a crime will be found on that email account, which is what the Fourth Amendment requires." Def. Reply at 2. But Barnes's argument reflects an overly narrow conception of what might constitute relevant evidence of her alleged crimes. A warrant may, for example, authorize the seizure of "evidence relevant to the *mens rea* element of the crime." *Walczyk v. Rio*, 496 F.3d 139, 159 (2d Cir. 2007); *see also United States v. Cohan*, 628 F. Supp. 2d 355, 364–65 (E.D.N.Y. 2009) (noting that even "innocent" business records may "contain[] material evidence of" a crime and thus be subject to seizure). Although Barnes disputes the Government's claim that her knowledge of the federal voucher programs and their terms would tend to make the *mens rea*

element of the charges against her “more . . . probable,” Fed. R. Evid. 401; Gov. Opp. at 7,² the Court concludes that such knowledge—for instance, knowing that Workforce1 employees approved voucher recipients and might therefore be fruitful targets for kickback payments—would, in fact, be relevant. And emails about the voucher programs could demonstrate such knowledge. Therefore, because the warrant authorized the seizure of “evidence . . . of violations” of the relevant statutes, Harris Decl. Ex. C, there was a “nexus between the items sought”—evidence of the alleged violations—and “the ‘particular place’ to be searched.” *Clark*, 638 F.3d at 95 (quoting *Stanford*, 379 U.S. at 481).

The Google Account is subject to a similar analysis. Agent Wilson’s warrant application stated that L&B’s website “currently lists” the Google Account “as its contact e-mail,” and that the website also “contains a scroll referencing ‘GOVERNMENT PROGRAMS,’ ‘WORKFORCE,’ and ‘ITA VOUCHERS.’” Harris Decl. Ex. C ¶ 19. According to Barnes, the fact that the Google Account was listed on L&B’s website in 2013 is insufficient to establish a “temporal connection” with her alleged crimes because “the complaint charges a conspiracy between 2009 and 2012.” Def. Br. at 8. She further claims the website actually referred to “VESID WORKFORCE,” a program that, unlike Workforce1, is designed to provide vocational training for individuals with disabilities.³ Def. Reply at 3.

² The Government actually cites “Fed. R. Evid. 1,” which does not exist.

³ Barnes is correct that false or misleading statements in affidavits are “troubling.” *United States v. Mankani*, 738 F.2d 538, 545 (2d Cir. 1984). However, as in *Mankani*, “there is no direct evidence that omissions, if any, were intentionally or recklessly made,” and as discussed in the text, Judge Ellis “still would have been justified in issuing the warrant” based on other statements in the warrant application. *Id.* at 546; *see also Franks v. Delaware*, 438 U.S. 154, 156 (1978) (holding that to find a warrant invalid based on a misstatement in the application, the false statement must have been “necessary to the finding of probable cause”).

Those arguments are unpersuasive. The fact that L&B's website referenced "GOVERNMENT PROGRAMS" in general, combined with the warrant application's numerous allegations involving L&B's participation in the Workforce1 voucher program specifically, provides a sufficient basis for concluding that L&B might have been participating in that program as of the date of the website's publication. There was thus a "fair probability" that the Google Account, which was listed on the website, would contain communications concerning L&B's involvement in the program. The fact that Agent Wilson accessed the website in 2013 does not affect that conclusion. Barnes asserts that L&B did not receive any Workforce1 vouchers after 2010. Def. Br. at 9. However, because Barnes is charged with conspiracy, it was appropriate for the Government to search for evidence of an agreement allegedly lasting from 2009 to 2012, Compl. ¶ 1; *see also United States v. LaSpina*, 299 F.3d 165, 173 (2d Cir. 2002) ("[T]he scope of the conspiratorial agreement . . . determines . . . the duration of the conspiracy." (quoting *Grunewald v. United States*, 353 U.S. 391, 397 (1957))), as Barnes effectively concedes, *see* Def. Br. at 8 ("[T]he Government has not alleged any criminal conduct by Ms. Barnes in 2013. The complaint charges a conspiracy between 2009 and 2012."). Indeed, the Complaint—which was attached as "Exhibit A" to the warrant application—details two conversations about vouchers between an individual alleged to be Barnes and a cooperating witness, which took place in 2012. Compl. ¶¶ 12, 13. Common sense suggests that websites are not inevitably updated, nor email addresses changed, on a year-to-year basis. Therefore, the fact that the Google Account appeared on L&B's website in 2013 created probable cause to search the account for communications regarding vouchers.

As Barnes points out, some warrant applications include specific emails sent from the target account, which were lacking here, *see United States v. McDarrah*, No. 05 Cr. 1182 (PAC),

2006 WL 1997638, at *9–10 (S.D.N.Y. Jul. 17, 2006); *United States v. Bowen*, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (Sand, J.), and the warrant application never actually alleges that Barnes used the email account to communicate about vouchers. However, Barnes provides no authority supporting her assertion that such evidence is *necessary*—indeed, the Fourth Amendment does not require “direct evidence” that the objects specified in the warrant will be found in the location to be searched, *Singh*, 390 F.3d at 182—and the cases she cites are inapposite. In *McDarrah*, the defendant had solicited an FBI agent posing as a minor, and the warrant application included incriminating emails sent to the agent from the defendant’s account. *See* 2006 WL 1997638, at *9. Requiring similar evidence in every case would ignore the fact that investigators do not always communicate with the defendant by email before they apply for a search warrant. Moreover, in affirming the *McDarrah* court’s denial of the defendant’s suppression motion, the Second Circuit clarified that a warrant “need not be limited to a location where the conduct amounting to evidence of wrongdoing . . . has already been uncovered, as long as there is a sound basis to conclude that evidence of wrongdoing may be found in additional specified locations.” *United States v. McDarrah*, 351 F. App’x 558, 561 (2d Cir. 2009) (citing *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006)). The question is whether there is a “fair probability” that evidence will be found in the account, *Travisano*, 724 F.2d at 346, not whether evidence has already been found there.

Bowen is even less supportive of Barnes’s position. In that case, the evidence of specific emails sent from the target account primarily figured not into the court’s inquiry regarding whether there was probable cause to search the account, but rather into its analysis of whether the Government was entitled to seize the *entire* account under the so-called “all-records” exception. *See Bowen*, 689 F. Supp. 2d at 684 (“Defendants’ enterprise was so pervaded with

criminal activity, and the target e-mail accounts were such essential instrumentalities of that enterprise, that seizure of the entire account was appropriately authorized pursuant to the all records exception.”). As discussed in more detail below, that analysis is not relevant to this case, because the warrants limited the items to be seized to evidence of specific listed crimes.

In sum, the Court concludes that the warrant application provided a “fair probability” that both the Yahoo Account and the Google Account contained evidence of the criminal conduct with which Barnes was charged, so there was probable cause to search the accounts.

2. The Warrants Were Sufficiently Particularized

The Fourth Amendment’s particularity requirement “prevents the seizure of one thing under a warrant describing another.” *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)). In order to satisfy this requirement, a warrant must include: (1) the specific offense for which the police have established probable cause; (2) a description of the place to be searched; and (3) the items to be seized, identified by their “relation to designated crimes.” *Id.* at 445–46 (quoting *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010)) (internal quotation mark omitted). The Government asserts that Barnes’s particularity arguments are limited to challenging the two-step search protocol authorized by the warrant. Gov. Opp. at 8. As discussed below, that assertion is not entirely accurate, but the Court will discuss the search protocol first.

Both warrants have two sections related to seizure: they first list information to be “disclosed” by the ISPs, and then list information to be “seized by the Government.” Harris Decl. Ex. D. The information subject to disclosure is broader than the information subject to seizure: the former category comprises “all stored electronic mail and other stored content information presently contained in” the two accounts, as well as non-content information, while

the latter is limited to “all information described above” (*i.e.*, in the “disclosure” section) “that constitutes fruits, evidence and instrumentalities” of the specified statutory violations. *Id.* As described in the warrant application, the ISPs would first make digital copies of all the information subject to disclosure and then turn that information over to the Government, after which Government investigators planned to “cursorily inspect all information from the accounts in order to ascertain what items of information contain evidence” of the charged crimes. Harris Decl. Ex. C ¶ 25.

Barnes’s basic argument is that even if the limitations on the scope of the seizure would render that seizure, standing alone, permissible under *Galpin*, the fact that the ISPs first disclosed to the Government *all* of the information listed in the warrants’ “disclosure” sections—essentially, the entire contents of the two email accounts—made the procedures authorized by the warrants “tantamount to a general search.” Def. Br. at 11. The Court disagrees.

Barnes’s argument is not without intuitive appeal, and the Court is conscious that searches involving stored digital content raise unique privacy concerns. *Cf. Galpin*, 720 F.3d at 447 (“[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.”). However, the Supreme Court recognized long ago that searching for files is not like searching for tangible objects, because it is impossible to know whether a given file contains relevant evidence without looking at it. *See Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (“In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.”). The same is true with computer hard drives and, as in this case, email accounts. *See Bowen*, 689 F. Supp. 2d at 682 (“In a search for electronic

documents such as e-mails, ‘the actual content of a computer file usually cannot be determined until it is opened with the appropriate application software on a computer’ or until each file is analyzed by a program capable of searching the files for specific content.” (quoting *United States v. Lamb*, 945 F. Supp. 441, 458 (N.D.N.Y. 1996))). The Government is thus correct that the search protocol used in this case is not “remotely atypical,” Gov. Opp. at 8; *see Vilar*, 2007 WL 1075041, at *35 (“it is frequently the case with computers that the normal sequence of ‘search’ and then selective ‘seizure’ is turned on its head” (quoting *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004)) (internal quotation marks omitted)), and the mere fact that the warrants required the ISPs to initially disclose the entire contents of Barnes’s accounts to the Government does not render them invalid.

Likely recognizing as much, Barnes suggests that the Government should at least have put a “‘firewall’ team in place to review the first copy provided” by the ISPs. Def. Br. at 10. Although Barnes does not specify what such a team would look like, most courts have not required investigators to utilize specific procedures for searching through computer or email files for evidence that they are authorized to seize. *See, e.g., Vilar*, 2007 WL 1075041, at *37–38 (collecting cases). Barnes cites *United States v. Cioffi*, 668 F. Supp. 2d 385 (E.D.N.Y. 2009), for the proposition that third-party firewall teams can be helpful for preventing the Government from intruding on defendants’ privacy. Def. Br. at 11. However, *Cioffi* specifically did not require such a procedure; the court simply noted, in dicta, that a firewall team might be one way of addressing the privacy concerns implicated by computer searches, before proceeding to invalidate a warrant for failing to limit the seizure it authorized by reference to specific crimes—which is not true of the warrant in this case. *See id.* at 392. Indeed, the *Cioffi* court recognized that “the majority of courts to have considered the question have not required the government to

specify its search protocol in advance,” *id.*, and delegating an initial segregation function to a firewall team would accomplish just that by forcing the Government to specify the protocol that the team should use. This Court is disinclined to depart from the majority position: “a rule that does not require a computer search protocol avoids the courts getting into the business of telling investigators how to conduct a lawful investigation, something the courts are ill-equipped to do.” *Vilar*, 2007 WL 1075041, at *38. *But cf. United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009) (“Segregation and redaction must be either done by specialized personnel or an independent third party.”), *superseded on other grounds*, 621 F.3d 1162 (9th Cir. 2010) (en banc). Courts may remedy investigators’ illegal snooping by excluding any evidence thereby obtained, not by invalidating the entire warrants. *See Vilar*, 2007 WL 1075041, at *37; *see also United States v. Shi Yan Liu*, 239 F.3d 138, 142 (2d Cir. 2000) (“the extreme remedy of blanket suppression should only be imposed in the most extraordinary of cases” (quoting *United States v. Foster*, 100 F.3d 846, 852 (10th Cir. 1996)) (internal quotation marks omitted)). Accordingly, the fact that the warrants did not prescribe a firewall team does not make them constitutionally infirm.

Apart from challenging the search protocol, Barnes makes two other arguments regarding particularity. First, although for the most part Barnes does not dispute that the warrants satisfied *Galpin*’s requirement that “the items to be seized” must be identified in “relation to designated crimes,” 720 F.3d at 446, she points out that the warrants authorized the seizure of “[e]lectronic mail, private messages, and other content concerning *smuggling*.” Def. Br. at 11 n.3 (emphasis added). The crimes with which Barnes is charged clearly do not involve smuggling, and the Government claims—and Barnes concedes—that the warrants’ nonsensical references were merely typographical errors. Yet because the warrant application did not provide grounds for

probable cause to seize evidence of smuggling, the warrants were invalid at least insofar as they authorized the Government to seize such evidence. *See Galpin*, 720 F.3d at 446 (“[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based.” (quoting 2 Wayne R. LaFare, *Search and Seizure* § 4.6(a) (5th ed. 2012)) (internal quotation marks omitted)). The next question is whether that matters.

The Government argues that the “e-mails at issue”—presumably, emails relevant to the actual charges in the Complaint—would have been seized in any event because the first clause of the warrants’ “seizure” sections authorizes the seizure of any information disclosed by the ISPs that constitutes “fruits, evidence and instrumentalities” of the statutory violations with which Barnes was charged. Because the information disclosed by the ISPs includes emails, the seizure of emails containing evidence of the charged crimes was therefore authorized even without the “smuggling” clauses. Gov. Opp. at 4–5 n.2. While not explicitly framed as such, this is effectively an argument that the warrants are “severable,” in other words, that evidence seized pursuant to their constitutionally infirm portions should be suppressed while evidence seized under their valid portions should be admitted. *See Galpin*, 720 F.3d at 448; *Vilar*, 2007 WL 1075041, at *38. The Court agrees that any evidence seized on the basis of the “smuggling” clauses may be suppressed without invalidating the warrants entirely.⁴

In *Galpin*, the Second Circuit adopted a severability test originally established by the Tenth Circuit. *See* 720 F.3d at 448 (citing *United States v. Sells*, 463 F.3d 1148, 1155–58 (10th

⁴ Notably, for the reasons discussed in the text, it is doubtful that evidence seized under the “smuggling” clauses would actually fall outside of the scope of warrants’ valid provisions: the warrants initially limit the Government’s seizure to evidence of violations of the correct statutes before they state that such evidence “includ[es]” certain kinds of content information related to smuggling. Harris Decl. Ex. D. In light of that fact, the Court’s severability analysis is designed chiefly to explain why the “smuggling” clauses do not invalidate the entire warrants.

Cir. 2006)). A court must first “separate the warrant into its constituent clauses,” then “examine each individual clause to determine whether it is sufficiently particularized and supported by probable cause,” and finally “determine whether the valid parts are distinguishable from the nonvalid parts.” *Id.* at 448–49. “In sum, the court must be able to excise from the warrant those clauses that fail the particularity or probable cause requirements in a manner that leaves behind a coherent, constitutionally compliant redacted warrant.” *Id.* at 449.

Under that standard, the warrants’ constituent clauses are separable, and their valid parts are distinguishable from their invalid parts. As the Government suggests, if one were to remove the “smuggling” clauses entirely, the warrants’ “seizure” sections would first authorize the seizure of all of the information disclosed by the ISPs—both content and non-content—that “constitutes fruits, evidence and instrumentalities of” the charged crimes. Harris Decl. Ex. D. After that initial clause, the warrants become clarificatory; excluding the “smuggling” clauses, they would provide merely that the seizure authorized by the initial clause “includ[es]” certain categories of information, such as transactional information, business records and subscriber information, and records of who “created, used, or communicated with” the accounts. *Id.* Although excising the “smuggling” clauses would thus remove a (perhaps helpful) clarification that the authorized seizure included “electronic mail, private messages, and other content information,” it would not affect whether the seizure of such information was, in fact, authorized. And because that authorization references the specific kinds of files described in the “disclosure” sections and is limited by reference to the crimes with which Barnes was charged, the remaining sections of the warrants are valid. See *Galpin*, 720 F.3d at 446; *United States v. Levy*, No. 11 Cr. 62 (PAC), 2013 WL 664712, at *9 (S.D.N.Y. Feb. 25, 2013); *United States v. Dupree*, 781 F. Supp. 2d 115, 148–49 (E.D.N.Y. 2011).

The cases cited by Barnes are readily distinguishable because, as even she characterizes them, they involved warrants that were “not limited by reference to the specific crimes charged.” Def. Reply at 4; *see United States v. Rosa*, 626 F.3d 56, 61 (2d Cir. 2010) (warrant “failed to state with any level of particularity the specific criminal activity alleged or the type of digital evidence to be sought”); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) (“Nothing on the face of the warrant tells the searching officers for what crime the search is being undertaken.”); *Cioffi*, 668 F. Supp. 2d at 396 (“The Warrant did not, on its face, limit the items to be seized . . . to emails containing evidence of the crimes charged in the indictment or, indeed, to any crimes at all.”). This case is different: again by Barnes’s own admission, the warrants “limit[] the ‘information to be seized’ to information that ‘constitutes fruits, evidence and instrumentalities of violations’ of 18 U.S.C. §§ 371 and 666.” Def. Br. at 9; *cf. United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) (“The search, in general, was limited to evidence of drugs and drug trafficking and, as it relates to the computer, was limited to the kind of drug and drug trafficking information likely to be found on a computer”).

It is true that the warrants did not on their “face” reference the charged crimes, but a supporting document can be used to “remedy a warrant’s lack of particularity” if it is “incorporated by reference in the warrant itself and attached to it.” *George*, 975 F.2d at 76; *see also Groh v. Ramirez*, 540 U.S. 551, 557 (2003) (holding that a supporting document that is not incorporated by reference cannot be used to remedy a warrant’s lack of particularity). A document is incorporated by reference when the warrant “direct[s] the executing officers to refer to the [document] for guidance concerning the scope of the search.” *George*, 975 F.2d at 76. In this case, the warrants refer to “attached riders,” and the riders indicate that the information subject to seizure relates to violations of “Title 18, United States Code, Sections 371 and 666.”

Harris Decl. Ex. D. An agent executing the warrants would therefore have had sufficient guidance, under *Galpin*, in determining which files were subject to seizure and which were not.

In any case, Barnes's primary argument concerning the "smuggling" clauses appears to be not that they rendered the warrants overbroad relative to the probable cause supporting them, but rather that references to smuggling might have confused the agents executing the warrants.

Def. Br. at 11 n.3. In support of that argument, she cites *United States v. Zemlyansky*, — F.

Supp. 2d —, 2013 WL 2151228 (S.D.N.Y. May 20, 2013), a scholarly recent opinion in which Judge Oetken held that a warrant with confusing provisions violated the Fourth Amendment.

However, those provisions furnished but one of several grounds for the warrant's invalidity, *see id.* at *11–17, and the nature of the confusion was meaningfully different. In *Zemlyansky*, the warrant contained two clauses concerning the seizure of electronic storage media; one was limited by reference to specific crimes, and the other was not. Therefore, had agents followed the latter clause, it would have resulted in "unlimited search and seizure" of certain kinds of storage media. *Id.* at *17. In this case, by contrast, everything that the warrants authorized the Government to seize was limited by their references to the charges against Barnes.

Barnes's final argument regarding particularity is that the warrants had no "temporal limitation." Def. Br. at 11. While it is true that "a number of out-of-circuit decisions . . . have found warrants for the seizure of business records constitutionally deficient where they imposed too wide a time frame or failed to include one altogether," *Cohan*, 628 F. Supp. 2d at 365–66, that position is not unanimous, *see id.* at 366 (collecting cases), and the Second Circuit has not addressed the issue.⁵ District courts in the Circuit appear to agree that the absence of a specified

⁵ In fact, *Galpin*'s failure to mention temporal limitations as a factor in its particularity analysis is notable in light of the fact that the warrant at issue in that case did not impose any such limitations. *See* 720 F.3d at 441–42.

time frame is at least relevant to particularity, *see, e.g., Zemlyansky*, 2013 WL 2151228, at *16; *United States v. Hernandez*, No. 09 Cr. 625 (HB), 2010 WL 26544, at *10–11 (S.D.N.Y. Jan. 6, 2010); *Cohan*, 628 F. Supp. 2d at 366; *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 58 (D. Conn. 2002), and they have considered the duration and complexity of the alleged scheme in assessing the importance of temporal limitations, *see Zemlyansky*, 2013 WL 2151228, at *16; *Hernandez*, 2010 WL 26544, at *10 (“The complexity and duration of the alleged criminal activities render a time frame less significant than in a case that required a search for a small set of discrete items related to one or only a few dates.”). As discussed above, Barnes concedes that she was charged with a conspiracy lasting several years, so her argument that the search should be limited to 2010—the year in which she received a suspiciously large number of vouchers—is not persuasive. In any case, the lack of Circuit guidance regarding the importance of time frames is a factor “trigger[ing] the ‘good-faith’ exception to the exclusionary rule.” *Cohan*, 628 F. Supp. 2d at 355.

3. The Good Faith Exception Applies

Although the Court has concluded that the warrants were supported by probable cause and were sufficiently particularized, the Government also argues that, even if the warrants were deficient, suppression would be unwarranted because the “good faith” exception and “all records” exceptions would apply. Gov. Opp. at 9 n.3. The Court agrees that, in the alternative, the good faith exception also forecloses Barnes’s suppression motion.

Under *United States v. Leon*, 468 U.S. 897 (1984), the exclusionary rule does not apply to “evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant” unless (1) the “issuing magistrate has been knowingly misled”; (2) the magistrate “wholly abandoned his or her judicial role”; (3) the warrant application is “so lacking in indicia

of probable cause as to render reliance upon it unreasonable”; or (4) the warrant is “so facially deficient that reliance upon it is unreasonable.” *Galpin*, 720 F.3d at 452 (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)). Behind this rule lies courts’ recognition that suppressing evidence of crimes imposes meaningful social costs, which are justified only if the Government’s conduct was “sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price.” *Zemlyansky*, 2013 WL 2151228, at *20 (quoting *Herring v. United States*, 555 U.S. 135, 144 (2009)).

Barnes claims that it was unreasonable for the Government to rely on a “warrant that wholly fails to connect the area to be searched with the alleged criminal activity.” Def. Reply at 8. This argument initially appears to suggest that the warrant itself was “facially deficient,” and that the fourth *Leon* exception should therefore apply. However, the Fourth Amendment “does not require that probable cause be stated in the warrant itself,” *Clark*, 638 F.3d at 103 (citing *United States v. Grubbs*, 547 U.S. 90, 98 (2006)), because whether probable cause exists is a question addressed by the magistrate who considers the warrant application, not by the agents who act on the warrant. *See Cohan*, 628 F. Supp. 2d at 364 n.4 (“the probable-cause analysis must be performed from the perspective of the magistrate who issued the warrant, to whom the supporting affidavit is . . . presented” (citation omitted)). Therefore, the warrants’ failure to contain indicia of probable cause cannot render them facially deficient. Nor can the fact that they failed to include a temporal limitation, given the lack of Circuit guidance on whether such limitations are in fact required. *See Cohan*, 628 F. Supp. 2d at 355

In any case, it is clear that Barnes’s real argument is that the warrant *application* did not sufficiently connect the email accounts to Barnes’s criminal activity, thus triggering the third *Leon* exception. She cites *United States v. Moran*, 349 F. Supp. 2d 425 (N.D.N.Y. 2005), in

which the court held that the good faith exception did not apply because “no facts in the [warrant] application connected the alleged criminal activity with” the place to be searched. *Id.* at 482. Where there are no such facts, a magistrate’s probable cause determination is so utterly unfounded as to both render reliance upon the resulting warrant unreasonable and suggest that the Government actually intended to mislead the magistrate. *See Clark*, 638 F.3d at 103 (noting that *Leon*’s third exception is implicated “most frequently . . . when affidavits are bare bones, *i.e.*, totally devoid of factual circumstances to support conclusory allegations”). In this case, however, the warrant application included at least *some* facts connecting the items sought with the place to be searched: it stated that the Yahoo Account and the Google Account were listed on DOL paperwork and L&B’s website, respectively. *See Harris Aff. Ex. C.* ¶¶ 18, 19. (Indeed, those facts were sufficient for both Judge Ellis and this Court to conclude that probable cause to search the accounts existed.) Under such circumstances, “a reasonable officer [may] rely upon the issuing magistrate’s determination that the facts were sufficient to support probable cause.” *Moran*, 349 F. Supp. 2d at 477; *see also Clark*, 638 F.3d at 104 (noting that “[i]t is the magistrate’s responsibility to determine whether the officer’s allegations establish probable cause,” so “[i]n the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination” (first alteration in original) (quoting *Leon*, 468 U.S. at 921) (internal quotation marks omitted)).

Additionally, while Barnes points out that Agent Wilson arguably misled Judge Ellis by claiming that L&B’s website’s scroll read simply “WORKFORCE,” as opposed to “VESID WORKFORCE,” Def. Reply at 8, an apparent falsehood in a warrant application must be “knowing or reckless” in order for suppression to be warranted. *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996). While recklessness may be inferred if the “omitted information was

‘clearly critical’ to assessing the legality of a search,” *id.* (quoting *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991)), that standard has not been met in this case. As discussed above, Agent Wilson pointed to sufficient additional evidence suggesting that the email accounts might contain communications about Workforce1 vouchers—including L&B’s website’s references to “GOVERNMENT PROGRAMS” and the Complaint’s allegations about L&B’s participation in the Workforce1 program specifically—such that his affidavit’s reference to “WORKFORCE” was not central to whether the warrants were ultimately supported by probable cause.

In sum, the Government’s conduct in obtaining the warrants was not so “flagrant” or “culpable” as to require deterrence. *Clark*, 638 F.3d at 104 (quoting *Herring*, 129 S. Ct. at 702) (internal quotation marks omitted). Therefore, even if the Court had concluded that the warrants were invalid, Barnes’s motion to suppress would be denied.

B. Barnes’s Motion for a Bill of Particulars Is Denied

Barnes also asks the Court to compel the Government to produce a bill of particulars pursuant to Federal Rule of Criminal Procedure 7(f). Generally, a bill of particulars is intended to “enable[] a defendant to prepare for trial, to prevent surprise, and to interpose a plea of double jeopardy should he be prosecuted a second time for the same offense,” *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 93, 150 (2d Cir. 2008) (quoting *United States v. Rigas*, 490 F.3d 208, 237 (2d Cir. 2007)) (internal quotation marks omitted), and “is required only where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused,” *Zemlyankys*, 2013 WL 2151228, at *36 (quoting *United States v. Chen*, 378 F.3d 151, 163 (2d Cir. 2004)) (internal quotation mark omitted). Whether to grant a bill of particulars is “within the sound discretion of the district court.” *Id.* (quoting *United States v. Panza*, 750 F.2d 1141, 1148 (2d Cir. 1984)).

In exercising their discretion, courts consider “the totality of the information available to the defendant—through the indictment, affirmations, and general pre-trial discovery—and determine whether, in light of the charges that the defendant is required to answer, the filing of a bill of particulars is warranted.” *United States v. Bin Laden*, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000). “The important question is whether the information sought is necessary, not whether it is helpful.” *United States v. Molina*, No. 11 Cr. 528 (JFK), 2013 WL 2455922, at *4 (S.D.N.Y. June 5, 2013) (quoting *United States v. Facciolo*, 753 F. Supp. 2d 449, 451 (S.D.N.Y. 1990)) (internal quotation marks omitted). If the defendant “has been given adequate notice of the charges against him, the government is not required to disclose additional details.” *United States v. Gibson*, 175 F. Supp. 2d 532, 536 (S.D.N.Y. 2001) (quoting *United States v. Payden*, 613 F. Supp. 800, 816 (S.D.N.Y. 1985)). Moreover, “[a] bill of particulars is not necessary where the government has made sufficient disclosures concerning its evidence and witnesses by other means.” *United States v. Walsh*, 194 F.3d 37, 47 (2d Cir. 1999).

As to the level of detail required to provide “sufficient disclosure” to the defense, “[t]here is no general requirement that the government disclose in a bill of particulars all the overt acts it will prove.” *United States v. Martoma*, No. 12 Cr. 973 (PGG), 2013 WL 2435082, at *5 (S.D.N.Y. June 5, 2013) (quoting *United States v. Carroll*, 510 F.2d 507, 509 (2d Cir. 1975)). Indeed, “Courts have routinely denied requests for bills of particulars concerning the ‘wheres, whens and with whoms’ of the crime.” *United States v. Bonventre*, No. 10 Cr. 228 (LTS), 2013 WL 2303726, at *6 (S.D.N.Y. May 28, 2013).

In this case, Barnes has already received copies of the Complaint, the Indictment, the warrants, and the warrant application. Harris Decl. ¶¶ 4, 6, 7. Also, during discovery, the Government provided Barnes with “documents relating to six vouchers it claims were

improperly obtained” and a “list of all vouchers ever received by [L&B].” Harris Decl. ¶ 8; *see* Harris Decl. Ex. G. In addition to that information, the defense requests “(1) the dates and amounts of the kickback payments allegedly made”; (2) the identities of persons “to whom the payments were allegedly made”; and (3) the identities of “students who were supposedly steered to [L&B] as a result of the payments.” Harris Decl. Ex. F.

However, the documents that the Government has provided already enable Barnes to obtain much of the information that she seeks. First, the Complaint indicates that the amount of each kickback payment was \$400. Harris Decl. Ex. A ¶¶ 11(a), 12(a). Second, the list of all the vouchers that L&B received includes the dates on which the vouchers were approved, thereby providing Barnes with approximate time frames for the alleged kickback payments. Harris Decl. Ex. G. Third, Barnes has been able to identify at least one person who is likely to testify that he received some of the alleged kickbacks—“Craig Burton (referred to in the Complaint as ‘CW #1’).” Def. Br. at 1. The fact that Barnes has been able to obtain some of the particulars she seeks through the information provided during discovery suggests that a bill of particulars is not warranted. *See Walsh*, 194 F.3d at 47.

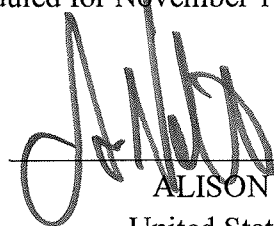
Moreover, the requested particulars concern the “whens” and “with whoms” of the crime. *Bonventre*, 2013 WL 2303726, at *6. Such details are not necessary for Barnes to prepare her defense. Because the documents that the Government has provided are sufficient to provide Barnes with notice of the crimes for which she has been charged, *see Gibson*, 175 F. Supp. 2d at 536, her request for a bill of particulars is denied.

III. CONCLUSION

For the foregoing reasons, Barnes's motions are DENIED. Trial in this case is set for November 4, 2013. Pursuant to the Court's order dated September 9, 2013, Dkt. No. 30, any 404(b) and *in limine* motions are due October 21, 2013, with opposition briefs due on October 28, 2013. The final pre-trial conference is scheduled for November 1, 2013, at 10:00 AM.

SO ORDERED.

Dated: October 21, 2013
New York, New York


ALISON J. NATHAN
United States District Judge